CLAIMS

1. An authentication system, comprising:

a portable recording medium which a forwarding agent has;

an authentication apparatus operable to verify authenticity of a visit by the forwarding agent, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent; and

an input/output apparatus operable to perform inputting and outputting of information between the portable recording medium and the authentication apparatus, the input/output apparatus being provided at an entrance of the residence, wherein

the portable recording medium stores therein in advance at least one piece of information concerning authenticity of the visit by the forwarding agent, and

the authentication apparatus stores therein at least one piece of information used for verifying authenticity of the visit by the forwarding agent, and judges whether or not the visit by the forwarding agent is authentic by, via the input/output apparatus, performing an authentication using the information stored in the portable recording medium and the information stored in the authentication apparatus.

2. The authentication system of Claim 1, wherein

the portable recording medium is an IC card,

the input/output apparatus is a card reader for the IC card,

the card reader detects a lock status of an entrance door, and

the authentication apparatus performs the authentication

if the card reader detects that the entrance door is locked.

3. The authentication system of Claim 2, wherein

the IC card stores therein certification information that certifies authenticity of the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent,

the authentication apparatus stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, authentication information that is used to examine the certification information, and

the authentication apparatus performs, via the card reader, the authentication using the certification information and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic.

4. The authentication system of Claim 3, wherein

the IC card further stores therein first visit information that indicates a business of the visit by the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent,

the authentication apparatus further stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information, and

the authentication apparatus, if a result of the authentication using the certification information and the authentication information is positive, acquires the first visit information from the IC card via the card reader, judges whether or not the acquired first visit information matches the stored

second visit information, and if a result of the judgment is positive, judges that the visit by the forwarding agent is authentic.

5. The authentication system of Claim 4, wherein

the first visit information is first time information that indicates a time period for the visit by the forwarding agent,

the second visit information is second time information that indicates a time period for the visit by the forwarding agent, and

the authentication apparatus judges whether or not the first time information matches the second time information.

6. The authentication system of Claim 4, wherein

the first visit information is first business information that indicates a business of the visit by the forwarding agent,

the second visit information is second business information that indicates a business of the visit by the forwarding agent, and

the authentication apparatus judges whether or not the first business information matches the second business information.

7. The authentication system of Claim 4, wherein

the first visit information includes (i) first time information that indicates a time period for the visit by the forwarding agent and (ii) first business information that indicates a business of the visit by the forwarding agent,

the second visit information includes (iii) second time information that indicates a time period for the visit by the

forwarding agent and (iv) second business information that indicates a business of the visit by the forwarding agent, and

the authentication apparatus judges whether or not the first time information matches the second time information, and judges whether or not the first business information matches the second business information.

8. The authentication system of Claim 4, wherein

the IC card further stores therein article information concerning an article delivered by the forwarding agent, and

the authentication apparatus further acquires the article information from the IC card via the card reader, and if the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the article information.

9. The authentication system of Claim 8, wherein

the article information is a name of a sender of the article, and

the authentication apparatus acquires the name of the sender from the IC card and displays the acquired name.

10. The authentication system of Claim 8, wherein

the article information is a name of the article, and

the authentication apparatus acquires the name of the article from the IC card and displays the acquired name of the article.

11. The authentication system of Claim 8, wherein

the article information is a message from a sender of the

article, and

the authentication apparatus acquires the message from the IC card and displays the acquired message.

12. The authentication system of Claim 4, wherein

the IC card further stores therein visitor information for identifying a visitor,

the authentication apparatus further acquires the visitor information from the IC card via the card reader, and if the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the visitor information.

13. The authentication system of Claim 12, wherein

the visitor information is a name of the visitor, and

the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor.

14. The authentication system of Claim 12, wherein

the visitor information is an image of a facial photo of the visitor, and

the authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo.

15. The authentication system of Claim 12, wherein

the visitor information is a name and an image of a facial photo of the visitor, and

the authentication apparatus acquires the name and the image

of the facial photo of the visitor from the IC card and displays the acquired name and image of the facial photo.

16. The authentication system of Claim 4, wherein

the authentication apparatus and the IC card perform a challenge-response authentication process using the certification information and the authentication information.

17. The authentication system of Claim 16, wherein

the certification information is an encryption key,

the authentication information is a decryption key,

the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the encryption key, and outputs the generated response data to the authentication apparatus via the card reader, and

the authentication apparatus receives the response data from the IC card, generates decrypted data by decrypting the response data using the decryption key, and performs an authentication by judging whether or not the generated decrypted data matches the challenge data.

18. The authentication system of Claim 17, wherein

the encryption key is holder certification information that shows biometric characteristics of a holder of the IC card, and

the authentication apparatus further receives holder

authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the decryption key.

19. The authentication system of Claim 17, wherein

the authentication apparatus is connected, via a network, to a distribution apparatus that distributes the decryption key,

the authentication apparatus receives the decryption key distributed from the distribution apparatus and stores the received decryption key prior to the visit by the forwarding agent.

20. The authentication system of Claim 16, wherein

the authentication information is a secret key,

the IC card stores therein a first key that is obtained by executing a one-way function on a key that is identical with the secret key,

the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the first key, and outputs the generated response data to the authentication apparatus via the card reader, and

the authentication apparatus receives the response data from the IC card, generates a second key by executing a function, which is identical with the one-way function, on the secret key, generates decrypted data by decrypting the response data using the second key, and performs an authentication by judging whether

or not the generated decrypted data matches the challenge data.

21. The authentication system of Claim 16, wherein

the authentication information is a first secret key,

the IC card stores therein a second secret key that is identical with the first secret key,

the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

the IC card receives the challenge data from the authentication apparatus, generates response data by encrypting the challenge data using the second secret key, and outputs the generated response data to the authentication apparatus via the card reader, and

the authentication apparatus receives the response data from the IC card, generates encrypted data by encrypting the challenge data using the first secret key, and performs an authentication by judging whether or not the generated encrypted data matches the response data.

22. The authentication system of Claim 16, wherein

the certification information is a secret key,

the authentication information is a public key that corresponds to the secret key,

the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

the IC card receives the challenge data from the authentication apparatus, generates a digital signature of the

received challenge data using the secret key, and outputs the generated digital signature as response data, to the authentication apparatus via the card reader, and

the authentication apparatus receives the response data from the IC card, and then performs an authentication by performing a signature verification on the received digital signature using the public key and the challenge data.

23. The authentication system of Claim 22, wherein

the secret key is holder certification information that shows biometric characteristics of a holder of the IC card, and

the authentication apparatus further receives holder authentication information that shows biometric characteristics of a visitor, and uses the holder authentication information as the public key.

24. The authentication system of Claim 16, wherein

the certification information is a secret key,

the authentication information is a public key that corresponds to the secret key,

the authentication apparatus generates challenge data, generates encrypted challenge data by encrypting the generated challenge data using the public key, and outputs the generated encrypted challenge data to the IC card via the card reader,

the IC card receives the encrypted challenge data from the authentication apparatus, generates response data by decrypting the received encrypted challenge data using the secret key, and outputs the generated response data to the authentication apparatus via the card reader, and

the authentication apparatus receives the response data from the IC card, and performs an authentication by judging whether or not the received response data matches the challenge data.

25. The authentication system of Claim 24, wherein

the IC card stores therein a public key certificate that is a proof of validity for the public key, which is also contained in the public key certificate, and

the authentication apparatus further acquires the public key certificate from the IC card, performs an authentication by judging whether or not the acquired public key certificate is authentic, and if a result of the authentication is positive, stores therein the public key that is contained in the public key certificate.

26. The authentication system of Claim 16, wherein

the IC card stores therein a second visit key that is identical with a first visit key that is distributed from the forwarding agent to the authentication apparatus prior to the visit,

the authentication apparatus further stores therein the first visit key,

if a result of an authentication by a challenge-response is positive, the authentication apparatus further generates visit examination data, and outputs the generated visit examination data to the IC card via the card reader,

the IC card receives the visit examination data from the authentication apparatus, generates encrypted visit examination data by encrypting the received visit examination data using the second visit key, and outputs the generated encrypted visit

examination data to the authentication apparatus via the card reader, and

the authentication apparatus receives the encrypted visit examination data from the IC card, decrypts the encrypted visit examination data using the first visit key, judges whether or not a result of the decrypting matches the visit examination data, and if it judges that the result of the decrypting matches the visit examination data, judges whether or not first visit information matches second visit information.

27. The authentication system of Claim 16, wherein

when the authentication apparatus outputs the challenge data to the IC card, the authentication apparatus converts the challenge data into converted challenge information that has the same contents as the challenge data but has a different data structure from the challenge data, and outputs, to the IC card, the converted challenge information as the challenge data.

28. The authentication system of Claim 27, wherein

when the IC card outputs the response data to the authentication apparatus, the IC card converts the response data into converted response information that has the same contents as the response data but has a different data structure from the response data, and outputs, to the authentication apparatus, the converted response information as the response data.

29. The authentication system of Claim 28, wherein

the converted challenge information is composed of one of an optical signal, a bar code, a QR code, an infrared signal,

and an audio signal, and

the converted response information is composed of one of an optical signal, a bar code, a QR code, an infrared signal, and an audio signal.

30. The authentication system of Claim 16, wherein

the authentication apparatus further stores therein an apparatus identifier for identifying the authentication apparatus itself,

the authentication apparatus outputs the apparatus identifier to the IC card via the card reader if the authentication apparatus judges that the visit by the forwarding agent is authentic, and

the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores therein the received apparatus identifier.

31. An authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium which the forwarding agent has, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent, the authentication apparatus comprising:

an information storage unit operable to store therein information used for the verifying of authenticity of the visit by the forwarding agent; and

a judgment unit operable to judge whether or not the visit by the forwarding agent is authentic by, via an input/output apparatus provided at an entrance of the residence, performing an authentication using information stored in the portable

recording medium concerning authenticity of the visit by the forwarding agent and using the information stored in the information storage unit.

32. The authentication apparatus of Claim 31, wherein

the input/output apparatus is a card reader for the recording medium,

the card reader detects a lock status of an entrance door, and

the judgment unit performs the authentication if the card reader detects that the entrance door is locked.

33. The authentication apparatus of Claim 32, wherein

the recording medium stores therein certification information that certifies authenticity of the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent,

the information storage unit stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, authentication information that is used to examine the certification information, and

the judgment unit performs, via the card reader, the authentication using the certification information and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic.

34. The authentication apparatus of Claim 33, wherein

the recording medium further stores therein first visit information that indicates a business of the visit by the forwarding

agent, as the information concerning authenticity of the visit by the forwarding agent,

the information storage unit further stores therein, as the information concerning verifying authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information, and

the judgment unit, if a result of the authentication using the certification information and the authentication information is positive, acquires the first visit information from the recording medium via the card reader, judges whether or not the acquired first visit information matches the stored second visit information, and if a result of the judgment is positive, judges that the visit by the forwarding agent is authentic.

35. The authentication apparatus of Claim 34, wherein

the recording medium further stores therein article information concerning an article delivered by the forwarding agent, and

the authentication apparatus further comprises:

an article information acquiring unit operable to acquire the article information from the recording medium via the card reader; and

an article information display unit operable to display the article information if the judgment unit judges that the visit by the forwarding agent is authentic.

36. The authentication apparatus of Claim 34, wherein

the recording medium further stores therein visitor information for identifying a visitor, and

the authentication apparatus further comprises:

a visitor information acquiring unit operable to acquire the visitor information from the recording medium via the card reader; and

a visitor information display unit operable to display the visitor information if the judgment unit judges that the visit by the forwarding agent is authentic.

37. The authentication apparatus of Claim 34, wherein

the authentication apparatus and the recording medium perform a challenge-response authentication process using the certification information and the authentication information.

38. The authentication apparatus of Claim 37, wherein

the authentication apparatus is a mobile phone.

39. A portable recording medium which a forwarding agent has and is used by an authentication apparatus operable to verify authenticity of a visit by the forwarding agent, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent, the portable recording medium comprising:

a storage unit operable to store therein in advance at least one piece of information concerning authenticity of the visit by the forwarding agent;

a receiving unit operable to receive first data from the authentication apparatus via an input/output apparatus provided at an entrance of the residence;

a data generating unit operable to generate second data from the first data using the information stored in the storage

unit, the second data being used for an authentication process; and

an output unit operable to output the second data to the authentication apparatus via the input/output apparatus.

40. The recording medium of Claim 39, wherein

the storage unit stores therein certification information that certifies authenticity of the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent, and

the data generating unit generates the second data using the certification information.

41. The recording medium of Claim 40, wherein

the storage unit further stores therein visit information that indicates a business of the visit by the forwarding agent, as the information concerning authenticity of the visit by the forwarding agent, and

the output unit further outputs the visit information to the authentication apparatus via the input/output apparatus.

42. The recording medium of Claim 41 further comprising

an article information storage unit operable to store therein article information concerning an article delivered by the forwarding agent, wherein

the output unit further outputs the article information to the authentication apparatus via the input/output apparatus.

43. The recording medium of Claim 41 further comprising

a visitor information storage unit operable to store therein visitor information for identifying a visitor, wherein

the output unit further outputs the visitor information to the authentication apparatus via the input/output apparatus.

44. The recording medium of Claim 41, wherein

the authentication apparatus stores therein authentication information that is used to examine the certification information, and

the authentication apparatus and the recording medium perform a challenge-response authentication process using the certification information and the authentication information.

45. The recording medium of Claim 44, wherein

the recording medium is attached to a mobile phone.

46. An authentication method for an authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium which the forwarding agent has, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent,

the authentication apparatus comprising:

an information storage unit operable to store therein information used for the verifying of authenticity of the visit by the forwarding agent, and

the authentication method comprising the step of:

judging whether or not the visit by the forwarding agent is authentic by, via an input/output apparatus provided at an entrance of the residence, performing an authentication using

information stored in the portable recording medium concerning authenticity of the visit by the forwarding agent and using the information stored in the information storage unit.

47. An authentication program that is run in an authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium which the forwarding agent has, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent,

the authentication apparatus comprising:

an information storage unit operable to store therein information used for the verifying of authenticity of the visit by the forwarding agent, and

the authentication program comprising the step of:

judging whether or not the visit by the forwarding agent is authentic by, via an input/output apparatus provided at an entrance of the residence, performing an authentication using information stored in the portable recording medium concerning authenticity of the visit by the forwarding agent and using the information stored in the information storage unit.

48. A computer-readable program recording medium that records therein an authentication program that is run in an authentication apparatus for verifying authenticity of a visit by a forwarding agent using a portable recording medium which the forwarding agent has, the authentication apparatus being provided in a residence of a person who is visited by the forwarding agent,

the authentication apparatus comprising:

an information storage unit operable to store therein

information used for the verifying of authenticity of the visit by the forwarding agent, and

the authentication program comprising the step of:

judging whether or not the visit by the forwarding agent is authentic by, via an input/output apparatus provided at an entrance of the residence, performing an authentication using information stored in the portable recording medium concerning authenticity of the visit by the forwarding agent and using the information stored in the information storage unit.